REMARKS

Before going into detail based on the enclosed Exhibits A, B, C and D, Applicant summarizes the main features of the claimed invention, which comprises a payload data stream comprising a header and a payload data block. The block is not any specific distribution of bits in the stream or anything else, but is a block which starts and ends in the payload data stream, which, in addition, has a header.

Importantly, the payload data block includes a first encrypted section and the second non-encrypted section. Both sections include audio data, video data, a combination of audio data and video data or binary data forming an executable program. The payload data in the encrypted first section is secured by the encryption feature, and, in accordance with the claimed invention (and this is a key feature), the data in the non-encrypted second section is also protected against manipulation due to the fact that, in the processing step, this data of the unencrupted second section is processed to deduce information characterizing this unencrypted second section of the payload data. Based on this information, a basic value is calculated, which is then encrypted.

To decrypt the payload data block, the output value is decrypted using a private key, for example. This results in the so-called "basic value." However, the basic value is not the payload data decryption key, but one needs to calculate the payload data key. This is done by processing the non-encrypted second section of the payload data block and to perform the linking step. This linking step then results in the payload data key. The complete decryption of the encrypted first section is possible, if the non-encrypted second section is authentic, *i.e.* was manipulated.

Then, there is a manipulation of the non-encrypted second section which is, in general, easily possible due to the fact that this second section is not encrypted.

The processing step in the decrypter (Claim 17) results in information which is different to process the information which is calculated by processing this non-encrypted second section on the encrypter-side. This difference is due to the manipulation of the non-encrypted second section.

In view of this manipulation, the "payload data key" calculated by the decrypter is different from the true payload data key used for encrypting on the encrypter-side, and decryption of the encrypted first section is no longer possible.

This means that the claimed invention is fully operative to detect a manipulation of the non-encrypted second section. Such a manipulation results in the situation that the decryption of the decrypted first section is not possible anymore. Thus, the payload data block is secured not only against unauthorized reading, due to the encrypted first section, but is also secured against manipulation due to the fact that the non-encrypted second section is processed, and this processing result is used for calculating the basic value which is then encrypted.

A further effect is that the processing load for an encrypter and, of course, for a decrypter can be reduced by only performing an encryption of a part of the payload data. However, the authenticity of the non-encrypted second is also secured due to the inventive feature.

Subsequently, Applicant discussed US 5,850,443 (the '443 patent) issued to Oorschot. Please refer to the attachment hereto labeled as Exhibit D. When considering Claim 1, and comparing Fig. 3 of the '443 patent to Claim 1, there is the following correspondence:

The step of generating a payload data key of Claim 1 corresponds to "create low-trust symmetric key" in the '443 patent. The payload data key is K'.

The "message" corresponds to "audio data, video data, a combination of audio data and video data or binary data forming an executable program" of Claim 1. The encrypting step corresponds "symmetric encryption" in Exhibit D. The step of processing corresponds to the hash 40 (X) operation, which is introduced before the block "leveling function". Hash 40 means that a hash is formed over the first 40 bits of the X-fields, as stated in column 6, line 59. The linking step corresponds to "leveling function" in Exhibit D, the encrypting step corresponds to "public-key encryption" to generate, for example A' as header field, and the entering step of Claim 1 is self-explanatory.

Importantly, however, there are differences between the '443 patent and Claim 1. Consider Exhibit A. Because Exhibit D additionally includes features of Nardone (US 5,805,700 – the '700 patent). The X-fields include the public key of A which has 512 bits and the encrypted leveled key. The encrypted leveled key is encrypted with the 512 bits key of A. This is outlined in column 6, line 59 where it is outlined that X is the concatenation of these two data fields.

The main features of Exhibit A, which shows definitely what is disclosed in the '443 patent, are that the complete message is encrypted, there is a plain text public key of A in the header, and the leveled key depends on the leading 40 bits of the public key in the first portion of the X-fields.

In view of that, the claim language in Claim 1 is new in view of US 6,175,626 (the '626 patent) for the following reasons:

Firstly, the third paragraph reads that "an encrypted section of said data block of the payload data stream is obtained rather than a completely encrypted payload data block.

Secondly, the third paragraph of Claim 1 furthermore reads that the second section of the payload data remains unencrypted.

Thirdly, in contrast to the '443 patent where the first 40 bits of the public key of A are processed by the hash 40 (X) function Claim 1 requires that the audio data, video data, a combination of audio data and video data or binary data forming an executable program of the unencrypted second section of the payload data are processed in the processing step.

Fourthly, the fifth paragraph of Claim 1 states that "said information", which is information generated in the processing step is linked to the payload data key. In contrast thereto, the leveling function in the '443 patent links information derived from the first 40 bits of the public key with the symmetric key K'.

In the Office Action, the Examiner only partly acknowledges these novel features. Specifically, the Examiner only states on page 4 that the '443 patent fails to disclose that the first and second sections include audio data . . . or the x-fields contain audio data. . .

The Examiner overlooks that only a section of the payload data block is encrypted.

Furthermore, the Examiner overlooks that the second section of the payload data remains unencrypted.

Additionally, the Examiner overlooks that the data in the unencrypted second section are processed, where the data in the second section are audio data . . .

Also, the Examiner overlooks that "said information" which stems from the processing of the unencrypted section are linked in the linking step.

Therefore, the Examiner's reasoning on page 4, first paragraph of the Office Action is faulty.

Now, the Examiner combines the '443 patent with the '700 patent. To this end, the Examiner referred again to Exhibit D and to Exhibit B, where Applicant has indicated a data stream which might occur when the combination proposed by the Examiner is performed.

Firstly, look at Exhibit D in a combination of the references as proposed by the Examiner, the second section of the message is not encrypted, bypasses the "symmetric encryption" block, and is directly written into the bit stream at the bottom of Exhibit D. The payload data block now only includes the encrypted first section, but does not include any additional encrypted data. The non-encrypted second section is now also in the payload data block.

However, and importantly, this combination does not result in applying the hash 40 function as outlined at 100 in Fig. 3 to the non-encrypted second section. Instead, the combination of the '443 patent and this '700 patent still means that the first 40 bits of the X-fields which are the first 40 bits of the public key of A are hashed, and the result is input into the leveling function block, as shown in Fig. 3.

Therefore, the conclusion is that the Examiner's combination of the '443 patent and the '700 patent does not result in the invention because this combination does not say that one has to hash the non-encrypted second section to deduce the information which is then used for leveling the symmetric key. Instead, the leveling operation is still done using a hash of the first 40 bits of the public key of A.

Therefore, with reference to the wording of Claim 1, the combination of the '443 patent and the '700 patent does not result in the step of processing the

audio data, video data, a combination of audio data and video data or binary data forming an executable program of the unencrypted second section to deduce information characterizing the unencrypted second section of said payload data, as defined in the fourth paragraph of Claim 1. This feature, which is introduced at 100 into Fig. 3, is definitely not attainable by the combination of the '443 patent and the '700 patent as indicated by the large cross at the 102 in Fig. 3, Exhibit D.

Furthermore, a combination of the '443 patent and the '700 patent does not disclose the linking step because "said information" and said payload data key are inked to obtain the basic value which corresponds to the "leveled key" in Fig. 3 of the '626 patent. Instead, the non-encrypted second section of the payload data block is never used for leveling anything in the combination of the '443 patent and the '700 patent.

Again, the leveled key as stated at Exhibit B depends on the leading 40 bits of the public key and does not depend on a non-encrypted second section of the payload data block as required by Claim 1.

Now, the Examiner produces a new reference, *i.e.* the '626 patent, and combines it with the other two references. The result of this combination is indicated at Exhibit C. A fair combination of Aucsmith with the other references is that the first portion of the X-fields, indicated by "public key of A with 512 bits," is replaced by Fig. 4 of the '626 patent. This means that instead of the public key of A with 512 bits, several additional information fields are included, such as version, serial number, signature algorithm identifier, issuer name, validity range, subject name, subject public key information and, additionally, extensions containing multimedia data. As indicated in Exhibit C all these information fields 402 to 416 would replace the public key of A with 512 bits as taught by the '443 patent and the second X-field which is the "encrypted leveled key" might still be there.

Now, the hash operation would take the first 40 bits which are, in a rough guess, probably fields 402, 404, 406, 408 for generating the information for the leveling function block in the '626 patent.

Alternatively, to be closer to the disclosure of the '443 patent, the hash function might use the first 40 bits of the subject public key information 414, which is nothing else than a public key of the subject, such as A. The result of this combination is quite similar to Exhibit B. Again, the leveled key does not depend on the non-encrypted second section in the payload data block, but depends on version, serial number, signature algorithm identifier, issuer name or on the first 40 bits of the subject public key information of the '626 patent

The Examiner refers to the extensions containing multimedia data in item 416. However, this extension(s) containing multimedia data is not included in the payload data block, but is included in the header. Furthermore, this extension is definitely different from the non-encrypted second section of the '700 patent, as discussed in connection with Exhibit B.

Furthermore, it would definitely not be a fair combination of the '700 patent with the '626 patent that one would replace a non-encrypted second section of the '626 patent by an extension containing multimedia data for the following reasons: The '626 patent teaches a non-encrypted second section which comprises certain frames of a video sequence. The '626 patent, however, teaches that these extensions containing multimedia data are used for authenticating the subject which has the subject public key. Column 4, line 65 reads as follows:

> "thus, the authentication information is used for authenticating multimedia information instead of providing access to directory services as in the prior art recommendation X.509, and is . . . . thus, also the multimedia extension(s), if any, contained in field 416 may provide stronger authentication, . . . field 416 may be used for any purposes according to an application requirement,

for example, for use of a credit card for payment during a transaction."

Video frames in a payload data block which, of course, belong to video frames in the payload data block which are encrypted, which is stated in column 1, lines 56 to 59 of the '700 patent can definitely not be replaced by authenticating multimedia pieces or any payment details, which do not have any relation to the payload at all or to the encrypted first section of the payload data block.

Therefore, the combination of the '443 patent, the '700 patent, and the '626 patent does not disclose the features in the step of processing and the features in the step of linking.

Technically speaking, as outlined in Exhibit C, a manipulation of the non-encrypted payload data cannot be detected because the operation 100 illustrated in Fig. 3 is not rendered obvious by the combination of all those three references.

In the claimed invention, however, a manipulation of the non-encrypted second section is detected as outlined above.

Therefore, the Examiner's conclusion and arguments in the Office Action are not technically correct and do not provide a proper basis for rejecting Applicant's claims for obviousness under 35 USC 103.

Further, with regard to the Examiner's statements on page 2, second paragraph, the Examiner outlines that all audio data, video data etc., are just a string of bits which can be interpreted, however, this is not justified. The term "audio data" implies that there was a certain audio format which is understandable by a certain audio rendering device. If the Examiner would try this for himself, he could load any text file onto his MP3 player, and the result would be only an error message. Therefore, text data is not audio data because

an audio processor cannot process the text data. The same is true for video data. When the Examiner introduces any text file or any binary string into his iPod or into his digital camera, he simply receives an error message because video data must be data which are so that a video processor can render this data. The same is true for binary data being an executable program. This is not any binary data, but has to be a certain executable file. If the Examiner, for example, wants to process a certain file in his Pentium computer processor, then nothing else but an error message occurs.

Therefore, one cannot display any string of bits on the computer screen and one can also not render audible any string of bits in an audio processor. Therefore, the Examiner's reasoning on page 2, second paragraph is not at all justified.

In view of the foregoing, the outstanding rejections are traversed and withdrawal thereof is indicated.

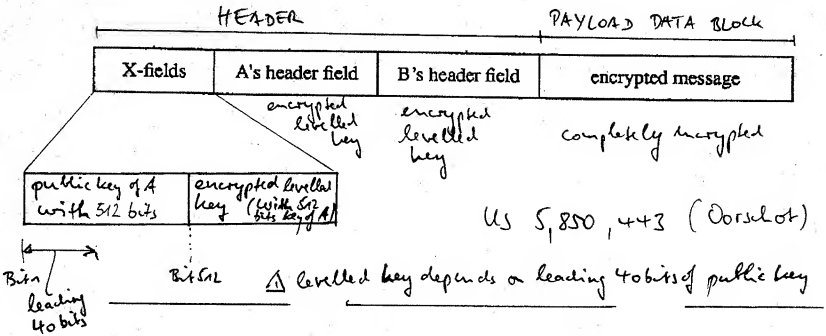
Should the Examiner deem it helpful, he is encouraged to contact Applicant's attorney at 650-474-8400.

Respectfully submitted,

Michael A. Glenn
Registration No. 30,176

Customer No. 22,262

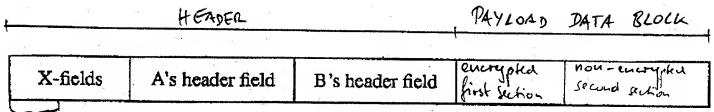
EXHIBIT A



US 5,850,443 (Dorsch et)

⚠ kerbelled key depends on leading 40 bits of public key

EXHIBIT B



↑ levelled key depends on leading 40 bits of public key

NOT on non-encrypted second section

US 5,850,448 (Dorsett)

AND

US 5,805,700 (Nardone)

EXHIBIT C

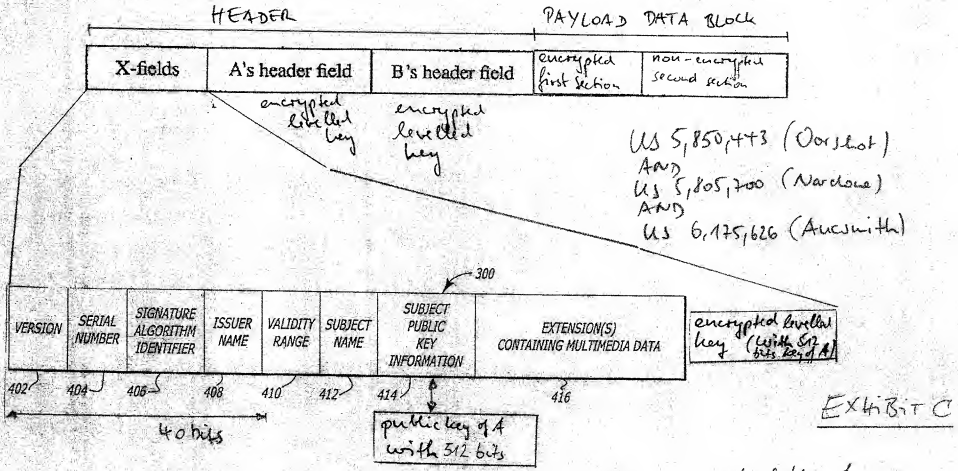

HEADER
PAYLOAD DATA BLOCK
X-fields
A's header field
B's header field
encrypted first section
non-encrypted second section
encrypted levelled key
encrypted levelled key
US 5,850,443 (Oorschot)
AND
US 5,805,700 (Nardone)
AND
US 6,175,626 (Alcorn)
300
VERSION
SERIAL NUMBER
SIGNATURE ALGORITHM IDENTIFIER
ISSUER NAME
VALIDITY RANGE
SUBJECT NAME
SUBJECT PUBLIC KEY INFORMATION
EXTENSION(S) CONTAINING MULTIMEDIA DATA
encrypted levelled key (with 512 bits key of A)
402
404
406
408
410
412
414
416
40 bits
public key of A with 512 bits
EXHIBIT C
Δ Levelled key does NOT depend on non-encrypted second section
In this combination, a manipulation of the non-encrypted payload data can not be detected. In the invention a manipulation will be detected.

EXHIBIT D

EXHIBIT D

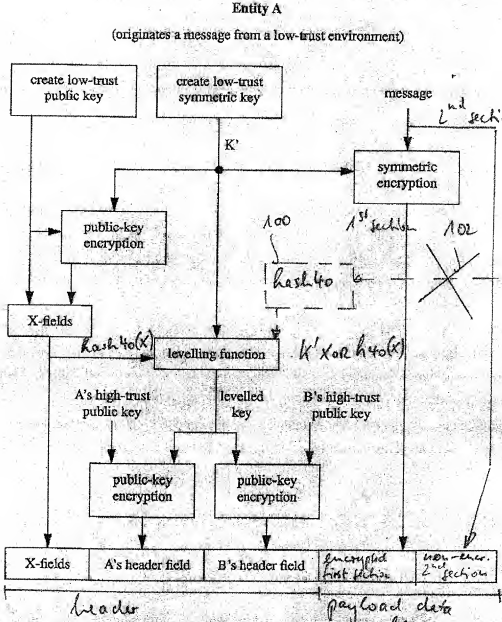


Figure 3